# PRIVACY ISSUES IN INTEGRATED PUBLIC SERVICES

**Charles D. Raab**
**University of Edinburgh**
**c.d.raab@ed.ac.uk**

# ESRC RESEARCH PROJECT: *PRIVACY AND DATA-SHARING IN MULTI-AGENCY WORKING* (RES/000/23/0158)

**Christine Bellamy & Perri 6 (Nottingham Trent University)**

**Charles Raab (University of Edinburgh)**

# GOVERNMENT POLICIES

- Joined-up government/better delivery of public services
  - Intensive and extensive use of personal data, including sharing across boundaries
- Protecting personal data/human rights
  - Greater personal control of information, including government transparency

# TENSIONS?

- Not inevitable: some say that good privacy protection can mean good information-sharing and good joined-up government
- But in practical decision-making contexts (e.g., health and social care, including child protection), there are tensions and conflicts between privacy and data sharing, and between running opposing *risks*

# WHAT ARE THE TENSIONS BETWEEN DATA-SHARING AND PRIVACY IN MULTI-AGENCY WORKING?

- Intensification of information sharing:
  - Commitment to major extension of e-government, 'joined-up government, service and data integration
  - Identity cards and population register (Citizen information Project), comprehensive database on children
  - Preventive approaches to managing risk
  - Targeted social intervention programmes
  - Desire for resource efficiency and effectiveness through discriminating judgments in social policies
  - Enhanced emphasis on citizen obligations

- Laws for privacy protection:
  - Implementation of European Directive 95/46/EC
  - Implementation of Data Protection Act 1998
  - Human Rights Act 1998
  - Common law of confidentiality

# WHAT ARE THE RISKS OF SHARING OR NOT SHARING DATA?

- Risks to dignity and risks to justice
- *'False negative'* judgment errors: no action taken, but ought to have been taken (if information had been shared): sometimes with adverse consequences
- *'False positive'* judgment errors: action taken, but ought not to have been taken (if privacy had been respected): sometimes with adverse consequences
- Current shift to intolerance of 'false negative' judgment errors and preference for action even if 'false positive' judgments are made

# HOW ARE THEY BEING MANAGED?

- Horizontal Strategies (generic, across government)
  - DPA 1998 and Information Commissioner
  - PIU Report (2002)
  - DCA's 'Toolkit' (2003)
  - Data standards and quality

- Vertical Strategies (specific, within sectors and partnerships; diversity)
  - Protocols
  - Codes of practice
  - Professional ethics
  - Training, roles and culture change

# DCA's 'TOOLKIT'

- Legal guidance on *vires* for sharing without consent
- Model protocol
- Codes of practice
- 'Trust Guarantee'
- Analytical Framework/Privacy Impact Assessment

# DEVELOPMENTS IN HEALTH CARE (UK)

- NHS Information Authority (NHSIA, to 4/05); now Connecting for Health; response to patchy ability to share patients' data in and around NHS; overcome legacy systems, poor implementation, non-integration
- National Programme for IT (NPfIT): many systems/procurement; centralised; £2.3 bn; IT and data standards; cradle-to-grave 'spine' summary patient record; Care Records Service, and other e-functions planned (booking, prescriptions, clinical decision tools); => sharing of records
- Confidentiality and privacy?

# KEY ISSUE: PURPOSES

- Are purposes specified so broadly that they may fall foul of the Data Protection Act 1998?
- How are purposes communicated to patients?
- Integration of care and non-care purposes?

# KEY ISSUE: CONSENT

- How can informed consent be ascertained?
- Costs of obtaining consent
- Segmented consent (‘sealed envelope’)
- Consistency of practice across sites

# KEY ISSUES: NECESSITY AND PROPORTIONALITY

- Who needs to know, and why?
- How much do they need to know?
- Routine access to databases

# PRIVACY AND CONFIDENTIALITY IN THE NHS: (I)

- Modern health practice requires new rules; doctor/patient confidentiality outmoded
- Caldicott Guardians in NHS agencies (1997; also in Social Care, 2001 +): senior staff in the NHS and social services appointed to protect identifiable patient information; protocols; 6 principles:
  - justify purpose
  - absolute necessity to use
  - minimum necessary
  - access strictly 'need to know'
  - awareness of responsibilities
  - understand and comply with law

# PRIVACY AND CONFIDENTIALITY IN THE NHS (II)

- *Confidentiality: NHS Code of Practice* (2003): privacy friendly 'confidentiality model' - addresses 'key issues'; disclosure (sharing) rules for different purposes (health care, non-health care, non-NHS); consent; 'sealed envelope'; 'no surprises'
- 'Role-Based Access Control' (RBAC)
- 'Care Record Guarantee'
- Subject Access ('MyHealthSpace')
- Patient Information Advisory Group (PIAG) and research use of information (Health ad Social Care Act 2001, 60)
- Information Commissioner's guidance (2002)

# LIMITS AND PROBLEMS

- Pressure on data protection principles from the way in which 'proportionality' and 'need to know' are construed in sharing information, and how consent is obtained
- In multi-agency working, potential inconsistency through 'vertical' variations in eliciting consent
- Gateways for data sharing are separate vertical settlements
- Uncertainty about need for primary legislation to grant powers to share
- Overtaken by events: further pressure for sharing and tolerance for 'false positive' judgment errors (e.g., in child protection)
- No settled 'horizontal' regulatory framework: *practitioners' judgments are inescapable*

# VARIATIONS IN JUDGMENTS

- Codes, protocols, rule interpretations inevitably leave room for judgment by practitioners
- Preliminary research findings in health, social care and policing show that sharing/confidentiality (privacy) judgments are shaped by variable (local) organisational settings, which influence the salience of rules and norms governing sharing/non-sharing of personal data
- Different propensity to take' false positive/false negative' risk also affects these decisions

# WIDER ISSUES

- Rules for data-sharing and privacy: too much and too formal?
- Blame: conflicting pressures on professionals?
- Data processing and sharing: too much for public trust?

# CONCLUSION

- To understand privacy and data-sharing in the public services (e.g., health), we need to know much more than what the laws require, permit or forbid
- We need to understand (and explain) *decision-making behaviour*; the constraints and opportunities within the decision-making contexts; why and how these vary; and what the consequences are for reconciling tensions between privacy and the sharing of personal information